Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Consumer Protection in the Broadband Era	)	WC Docket No. 05-271

Comments of VeriSign, Inc.

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Eric Rock
Director, Directory & Database Services
4501 Intelco Loop SE
Olympia, WA 98503
tel: +1 360.493.6190
mailto:erock@verisign.com

Michael Aisenberg
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6611
mailto:maisenberg@verisign.com

Brian Cute
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6615
mailto:bcute@verisign.com

Filed: 17 January 2006

1. As the largest independent provider of intelligent infrastructure services spanning both the legacy PSTN and IP-enabled Next Generation Networks, VeriSign is an interested party in this proceeding in areas that involve the secure availability and interoperability of authoritative directories containing CPNI.[1] Such directory capabilities are essential to the effectuation of consumer protection and an array of other public interest and national policy objectives. VeriSign urges that the Commission exercise its Title I and new *Preventing Cyberstalking* authority and require, as proposed in the NPRM and discussed below, necessary secure availability and interoperability of authoritative CPNI directory information for public network infrastructure and services regardless of the underlying technology.

I. AUTHORITATIVE CPNI DIRECTORIES AND COMMON TECHNICAL CAPABILITIES ARE CRITICAL FOR CONSUMER PROTECTION AND OTHER IMPORTANT PUBLIC INFRASTRUCTURE NEEDS

2. In the world of electronic communication networks, a ***directory*** is a database maintained by a service provider or a registrar of identifiers that show who has been assigned a particular number or identifier for a service. Examples include telephone numbers and Internet service names or addresses. For a specific identifier, the directory usually contains the user or subscriber name, contact addresses, and other information relevant to their service account or network connectivity. Directories may also exist for objects (physical or "virtual") such as equipment, consumer products, software, or protected content (movies, songs) that are associated with communication services and have a unique identifier.

3. An ***authoritative CPNI directory*** is the directory maintained by the entity – frequently a service provider - responsible by law, regulation, or industry practice for the allotment, assignment, or administration of unique communication identifiers. In the context of this proceeding, the authoritative CPNI directory is that maintained by a broadband Internet access provider in conjunction with all services offered. In many

---

[1] *See* para. 146 *et seq.*, *Notice of Proposed Rulemaking in matters of Consumer Protection in the Broadband Era*, WC Docket No. 05-271, FCC 05-150, released 23 Sept 2005 [hereinafter referred to as *Framework NPRM*].

communication networks today, there is a hierarchical ***chain of authority*** of organizations which allocate identifiers, first in a block (e.g., a contiguous IP address block) and then assigned from that block, then potentially sub-assigned again. Thus, in most cases, there is a pyramidal array of authoritative directories that are part of a hierarchical chain. Each party in this administrative process maintains an authoritative directory for those numbers they assign. The ability to rapidly discover the unique authoritative directory for a particular identifier within the hierarchy is a critical capability – whether an IP address, telephone number, or messaging name, depending on what services are bundled with Internet access.

4. CPNI Directories can be maintained in a great many different ways, and on different software platforms. In many cases, records maintained in CPNI directories contain protected, sensitive or valuable proprietary or personal information, which raise considerations of security and limitations on access and privacy. There also exists a substantial diversity of communication identifiers as well as hierarchical distribution responsibilities among large numbers of parties. CPNI directory interoperability is the ability for an authorized party (other than the service provider or identifier registrar) to interact with directory-based information in a consistent structured manner. This is most often accomplished with an open standards based query-response mechanism using a pre-defined information structure known as *syntax*. The better standards provide multiple features - especially authentication and auditing capabilities to enhance the integrity of the information and privacy.

5. Today's public communication networks and services make use of authoritative CPNI directory interoperability for almost everything performed as part of the services offered to subscribers, for the integrity and security of the networks and services, for commercial relationships with other service providers, and to meet government mandates, including consumer protection needs such as prevention of stalking. The needs range from mundane tasks such as contacting another party and billing, to advanced consumer protection services such as automatic roaming, callerID, fraud protection, and availability management. Authoritative directory interoperability is used among service providers and operators to collectively manage and troubleshoot their network facilities and services.

6. Reliable interoperability of authoritative CPNI directories is also a critical enabler for an array of longstanding government public policy requirements and services. These include provider competition, number portability, priority access, emergency warning, infrastructure protection, public safety, directory assistance, disability assistance, consumer protection, and assistance to law enforcement.

7. In addition to all other uses, including consumer protection, the capability is frequently used for law enforcement, homeland security, and national security officials in gathering and analyzing network forensic information for criminal, infrastructure protection, and terrorism investigations. CPNI directory capability is so important that international law enforcement assistance treaties and important national law specifically provide or rely on it for their effective implementation. The numerous examples include the U.S. Communications Assistance for Law Enforcement Act (CALEA) discussed below, the Prevention of Cyberstalking discussed below, the Convention on Cybercrime, and provisions of the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.

8. A complete summary of Authoritative CPNI directory interoperability requirements for IP-Enabled Next Generation Networks is depicted in Table 1, below. Many of these requirements have little or nothing to do with consumer protection; and depending on the degree of bundling of services together with broadband Internet access, may consist of CPNI directories maintained by third party providers. The list is divided into three sections: basic information associated with the service identifier, supplementary bundled services, and necessary features of the interoperability protocol that include essential consumer protection capabilities.

Category	Requirement	General Description
basic capability	**CPNI Service Identifier**	Authenticated directory associated with all CPNI Service Identifier implementations
supplementary capability	**Number Portability**	Information relevant to whether the CPNI Service Identifier is subject to porting and ancillary porting related information
	Priority Access	Subscriber special priviliges during times of emergency or network congestion
	Roaming	Subscriber automatic or manual agreements related to roaming clearing
	Quality of Service	Subscriber quality of service preferences
	Directory Assistance	Subscriber restrictions on availability of information to the public
	CallerID	Subscriber preferences concerning the availability of CallerID information to calling parties
	Disability Assistance	Subscriber disabilities pertinent to communication services
	Language preference	Subscriber's language preference
	Personal emergency (E112/911)	Subscriber information relevant to public safety officials during a personal emergency
	Public emergency alerts	Subscriber public emergency alert preferences
	DoNotCall	Subscriber preferences concerning unwanted solicitation communications
	Payment Methods	Subscriber preferences concerning manner of payment for services
	Intercarrier Compensation	Subscriber information relevant to intercarrier compensation
	Service Specification	Subscribers preferred default service provider(s)
	Application Interworking	Information relevant to interworking among subscriber applications
	Profile Management	Subscriber profile information made available to the public or to specific users
	Presence	Subscriber preferences concerning location and status
	Availability	Identity preference expressions
	Location	Subscriber geolocation
	Push Management	Subscriber's preferences concerning receipt of information based on geolocation
	Digital Rights Management	Subscriber's preferences and authorizations for receipt and use of intellectual property
	Device Management	Information relevant to the use of subscriber terminal devices
	Authentication Credentials	Subscriber digital certificates or other authentication information
	Information verification level	Extent to which basic subscriber has been verified and when
protocol feature	**Authentication**	Authentication requirements for queries
	Auditing	Auditing of queries, including accounting mechanisms
	Multiple Syntax Support	Query syntaxes accepted
	Mutiple Language Support	Languages supported
	Extensibility and Localisation Mechanisms	Means by which additional directory schemas and modules can be created, discovered, and appended to queries

Table 1. Authoritative CPNI Directory Interoperability Requirements

II. THE EXISTING AUTHORITATIVE CPNI DIRECTORY FRAMEWORK

9. Current requirements for authoritative CPNI directory interoperability have their origins in the breakup of AT&T in the early 1980s, and the realization that such interoperability was essential to bringing about an open, competitive telecom provisioning market. The requirements for the capabilities were mandated by the FCC in 1986 in the *Computer III Decision* and subsequently incorporated into Sec. 222 of the Communications Act of 1996.[2] In 1994, Congress also adopted Sec. 103 of the Communications Assistance for Law Enforcement Act (CALEA) which effectively mandates authoritative directory interoperability support capabilities in conjunction with enabling lawfully authorized electronic surveillance.[3]

10. In the early 1980s, the mainstream telecommunications and information systems industries – realizing the importance of authoritative integrated directory interoperability - collaborated on a common Open Systems Interconnection (OSI) directory standard known as X.500 and administrative arrangements for all names and objects. The marketplace, however, only partially embraced the approach. At about the same time, the adoption of the *Computer III Decision* caused a large-scale flurry of industry collaboration resulting in a set of Bellcore (now Telcordia) "GR" standards that provide the signaling system based authoritative CPNI directory interoperability in North America today. [4] During the 1990s, the growing need for IP-enabled directory interoperability resulted in attempts to graft capabilities onto native WHOIS and LDAP implementations (Referral WHOIS and Open LDAP), but were insufficient and little used.[5]

---

2 *See Report and Order*, CC Docket No. 85-229, Report and Order, 104 FCC 2d 958 (1986).

3 *See* 47 U.S.C. § 1002.

4 *See, e.g.*, Telcordia Technologies, Generic Requirements for GetData (A Module of FR-LIDB-1), Telcordia Technologies Generic Requirements, GR-2838-CORE, Issue 3, August 2002; Telcordia Technologies, LSSGR: CLASSSM Feature: Calling Name Delivery Generic Requirements (FSD 01-02-1070) (A Module of LSSGR, FR-64), Telcordia Technologies Generic Requirements, GR-1188-CORE, Issue 2 December 2000; Telcordia Technologies, Network Interface Specification (CCSNIS) Supporting Line Information Database (LIDB) Service (A Module of CCSNIS, FR-905, and FD-LECKIT-CD-01), Telcordia Technologies Generic Requirements, GR-954-CORE, Issue 3 December 2000.

5 See Referral Whois Protocol (RWhois)m RFC 1714, Nov 1994; Referral Whois (RWhois) Protocol V1.5, RFC 2167, June 1997; Open LDAP, <http://www.openldap.org/>

III. TITLE I AND *PREVENT CYBERSTALKING* AUTHORITY SHOULD BE EXERCISED TO REQUIRE TECHNOLOGY NEUTRAL COMPARABLE SECURE AVAILABILITY AND INTEROPERABILITY OF CPNI DIRECTORY INFORMATION

11. In competitive markets, legal mandates substitute for market-based incentives to provide critical services for which revenues are not normally compensatory to the businesses that must support them. Services such as universal CPNI directory interoperability solutions for public interest capabilities such as consumer protection and the other capabilities listed in Table 1, might not normally be offered (or offered only at fully allocated cost bases—and thus expensive prices) unless national policies embodied in law and regulation direct their availability. In addition, without legal mandates for CPNI directory interoperability, most providers of network services tend to protect their customer bases by restricting access to directory information. History has confirmed these tendencies – where the FCC's 1986 *Computer III Decision* subsequently created a fast-paced, innovative, competitive telecom directory interoperability services market in the U.S., the market elsewhere in the world developed much more slowly and less extensively for lack of such a mandate. In addition, Internet service providers may reduce expenses and tilt competitive playing fields by eliminating interoperable CPNI directory capabilities.

12. In the context of this proceeding dealing with the Commission's consumer protection framework for broadband IP access services, as well as other related proceedings where IP-enabled Next Generation Network frameworks are being developed, VeriSign urges exercise of Title I authority as necessary to assure interoperability and availability of authoritative CPNI directory services, including the unbundling of supplementary services listed in Table 1, above. Such action is also appropriate in assuring a technology neutral continuation of the important array of public policy, national security, and privacy objectives underlying Sec. 222 of the 1996 Act, Sec. 103 of CALEA, the USA Patriot Act, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.

13. The Commission now also has explicit authority as well as a mandate to act to require authoritative CPNI directory services pursuant to the new *Prevent Cyberstalking* provision recently adopted by Congress and signed into law by President Bush on 5 January 2006.[6] Section 223(h) of the Communications Act of 1934 was amended to extend consumer protection provisions to include "any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet."[7] The specific consumer protection provisions in Section 223(h) go to the failure to disclose one's identity in the course of an intentional communication "to annoy, abuse, threaten, or harass any person."[8] One of the principal mechanisms, and frequently the only way, to effectively implement the *Prevent Cyberstalking* provision is through the use of authoritative CPNI directory services providing the equivalent of CallerID.

14. The Commission in the instant NPRM "…ask[s] commenters to describe any technical, economic, or other impediments that may affect the ability of broadband Internet access service providers to comply with such regulations."[9] Just as they were in the years following the *Computer III Decision* on authoritative CPNI directory interoperability, the development and use of common industry protocols are critical to implementing any policy requirements. Fortunately, ongoing industry activity along these lines is already underway. Beginning around 2002, the telecom directory community began work on a powerful, multi-purpose XML and ASN.1 based directory interoperability standard culminating in the recent adoption and deployment of the ITU-T E.115v2 standard. About the same time in 2002, the Internet IETF community began work on a somewhat more limited XML based standard known as IRIS (Internet Registry

---

6 See H.R. 3402, *Violence Against Women and Department of Justice Reauthorization Act of 2005 (Enrolled as Agreed to or Passed by Both House and Senate)*, Public Law No. 109-162; President Signs H.R. 3402, the "Violence Against Women and Department of Justice Reauthorization Act of 2005," Office of the Press Secretary, The White House, Jan 5, 2006. See also, House Report 109-233 - Department of Justice Appropriations Authorization Act, Fiscal Years 2006 Through 2009

7 *Id.* at Sec. 113.

8 47 U.S.C. § 223(a)(1)(C).

9 *Framework NPRM* at para. 147.

Information Service) – with specific schema for IP address, domain name, and ENUM resolver systems (respectively, AREG, DREG, and EREG).[10]

15. Over the past several years, the expanding implementation of widespread broadband Internet access – increasingly combined with VoIP offerings - have resulted in major industry segments and government agencies worldwide focusing on the requirements for IP-enabled Next Generation Networks. This includes an ecosystem of standards activities, workshops, and regulatory proceedings. Particularly significant is the year-long effort of the White House National Security Telecommunications Advisory Committee (NSTAC) NGN Focus Group - whose report and recommendations are now expected in February. Authoritative CPNI directory availability and interoperability is a common denominator all of these activities – with a widespread recognition that the effective implementation of such directory capabilities is especially critical to the needs of consumers, as well as the maintenance, security, competitiveness, and success of national public IP-enabled infrastructures.

15. VeriSign urges the Commission to leverage both the current ongoing industry work and the twenty years of marketplace robustness, innovation, and consumer protection services stemming from the original *Computer III Decision*, by going forward with a consistent technology neutral framework for protected CPNI directory availability and interoperability. Such a framework would maintain the existing requirements as national policy for public communication infrastructures under Title I, while allowing industry the flexibility to implement the details through ongoing industry collaborative mechanisms. Such an action also seems effectively mandated by the new Title 47 *Prevent Cyberstalking* provision adopted by Congress.

---

[10] *See* ITU-T Recommendation E.115 - 2005, *Computerized directory assistance* [also referred to as E.115v2]; *Cross Registry Internet Service Protocol (CRISP) Requirements*, RFC 3707, Feb 2004;; *IRIS: The Internet Registry Information Service (IRIS) Core Protocol*, RFC 3981, Jan 2005. *See also*, ITU-T Study Group 17, Q2 Rapporteur Group on Directory Services, Directory Systems, and Public-key/Attribute Certificates, <www.itu.int/ITU-T/studygroups/com17/sg17-q2.html>; EIDQ, <www.eidq.org>; IRIS: the Cross Registry Information Service Protocol (crisp) charter, <www.ietf.org/html.charters/crisp-charter.html>.